Corr. to KR 2000-0049114

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－504137
（P2000－504137A）
(43)公表日　平成12年４月４日(2000.4.4)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ

審査請求　有　　予備審査請求　有　（全 29 頁）

(21)出願番号　特願平10－517883
(86)(22)出願日　平成９年９月15日(1997.9.15)
(85)翻訳文提出日　平成11年４月15日(1999.4.15)
(86)国際出願番号　ＰＣＴ／ＤＥ９７／０２０７０
(87)国際公開番号　ＷＯ９８／１６８８３
(87)国際公開日　平成10年４月23日(1998.4.23)
(31)優先権主張番号　１９６４２５６０．３
(32)優先日　平成８年10月15日(1996.10.15)
(33)優先権主張国　ドイツ（ＤＥ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＢＲ，ＣＮ，ＪＰ，ＫＲ，ＭＸ，ＲＵ，ＵＡ，ＵＳ

(71)出願人　シーメンス　アクチエンゲゼルシヤフト
ドイツ連邦共和国　Ｄ－80333　ミュンヘン　ヴィッテルスバッハープラッツ　２
(72)発明者　シュテファン　プファープ
ドイツ連邦共和国　Ｄ－82049　グロースヘッセローエ　ヴェターシュタインシュトラーセ　２
(74)代理人　弁理士　矢野　敏雄　（外３名）

(54)【発明の名称】　電子的データ処理回路

(57)【要約】
本発明は、マイクロプロセッサのような作動モジュール（１，１０１）と、少なくとも１つのデータメモリ（２，３，４，５，１０２，１０３，１０４，１０５）と、データメモリ（２，３，４，５，１０２，１０３，１０４，１０５）と作動モジュール（１，１０１）との間に延びているデータバス（１０６）とを有する電子的データ処理回路に関する。上位概念によるデータ処理回路においてメモリは屡々、できるだけアクセスすべきでない情報を含む。従って、電気的データ処理回路の操作に対する安全手段を講ずる必要がある。従って、本発明の課題とするところは、不都合な変化をさせないようにすべき改善された保護防止手段を有する上位概念による電気的データ処理回路を提供することにある。前記課題は、本発明により次のようにして解決される、即ち、データメモリ（２，３，４，５，１０２，１０３，１０４，１０５）と、データバス（１０６）との間の領域にて、及び／又は作動モジュール（１，１０１）とデータバス（１０６）との間の領域にて、少なくとも１つのエンコーディング、暗号化モジュール（２０～２２，

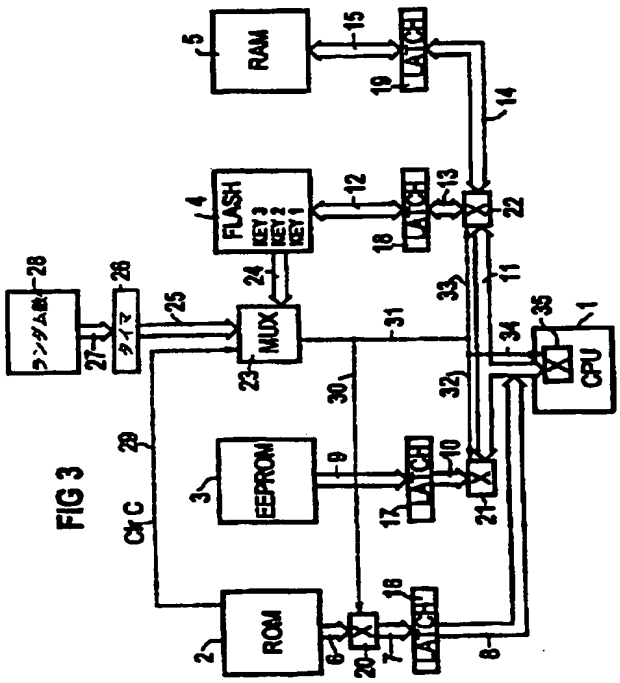

FIG 3

【特許請求の範囲】

1. マイクロプロセッサのような作動モジュールと、少なくとも１つのデータメモリと、データメモリと作動モジュールとの間に延びているデータバスとを有する電子的データ処理回路において、

データメモリ（２，３，４，５，１０２，１０３，１０４，１０５）と、データバス（１０６）との間の領域にて、及び／又は作動モジュール（１，１０１）とデータバス（１０６）との間の領域にて、少なくとも１つのエンコーディング、暗号化モジュール（２０～２２，３５，１０７）が設けられており、ここで前記エンコーディング、暗号化モジュール（２０～２２，３５，１０７）は、次のように構成されている、即ち、作動モジュール（１，１０１）とデータバス（１０６）との間の領域にて、ないし、データメモリ（２，３，４，５，１０２，１０３，１０４，１０５）と、データバス（１０６）との間の領域にて、エンコーディング、符号化及び／又はデコーディング、復号化が実施可能であるように構成されていることを特徴とする電子的データ処理回路。

2. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックがエンコーディングアルゴリズムを用いてエンコーディング可能であるように構成されていることを特徴とす

る請求の範囲１記載のデータ処理回路。

3. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックがハードウエアーエンコーディング、暗号化を用いてエンコーディング可能であるように構成されていることを特徴とする請求の範囲１又は２記載のデータ処理回路。

4. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックの個々のビットウエイトが選択的に変化可能であるように構成されていることを特徴とする請求の範囲３記載のデータ処理回路。

5. エンコーディング、暗号化モジュールは、少なくとも１つのＥＸＯＲ素子を有することを特徴とする請求の範囲４記載のデータ処理回路。

6. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７

）は、データバスのデータ線路の接続シーケンスが選択的に変化可能であるように構成されていることを特徴とする請求の範囲３から５までのうち１項記載のデータ処理回路。

7. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックが少なくとも部分的に遅延可能であるように構成されていることを特徴とする請求の範囲３から６までのうち１項記載のデータ処理回路。

8. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は少なくとも１つのキー鍵の入力のために少なくとも１つの入力側を有することを特徴とする請求の範囲３から７までのうち１項記載のデータ処理回路。

9. １つ又は複数のキー鍵がデータ処理回路の１つのフラッシュ（Ｆｌａｓｈ）ーセル内に格納されていることを特徴とする請求の範囲８記載のデータ処理回路。

10. キー鍵は、データ処理回路の収容のため、ＩＣ回路の埋込構造内に埋込まれていることを特徴とする請求の範囲８又は９記載のデータ処理回路。

11. キー鍵がそこに格納されている場所の操作スキャニングのためセンサ系が設けられていることを特徴とする請求の範囲８又は９記載のデータ処理回路。

12. データ処理回路は次のように構成されている、即ち、作動モジュールにより、所定の動作ないし演算実施の際、１つのキー鍵がエンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）内に入力可能であることを特徴とする請求の範囲８から１１までのうち１項記載のデータ処理回路。

13. ランダム発生器（２８）が設けられており、該ランダム発生器（２８）により、１つのキー鍵がランダムに選択可能であることを特徴とする請求の範囲８から１２までのうち１項記載のデータ処理回路。

14. 作動モジュール（１０１）にて使用されている１つのアドレスから１つのキー鍵を導出するための装置（１２０）が設けられていることを特徴とする請求の範囲８から１２までのうち１項記載のデータ処理回路。

15. 時間測定装置（２６）が設けられており、この時間測定装置（２６）により、キー鍵の入れ替えが導入可能であることを特徴とする請求の範囲８から１３までのうち１項記載のデータ処理回路。

16. 作動モジュール（１）及び少なくとも１つのデータメモリ（２，３，４，５）を結合するデータバスの少なくとも１つのデータ線路（７，８，３４，１１）の領域にて、少なくとも２つのエンコーディング、暗号化モジュール（１８，１９，２０，２１，３５）が設けられており、ここで、前記エンコーディング、暗号化モジュール（１８，１９，２０，２１，３５）は、次のように構成されている、即ち、エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）の共働により完全なエンコーディング、暗号化ないしデコーディング、復号化が実施可能であるように構成されていることを特徴とする請求の範囲１から１５までのうち１項記載のデータ処理回路。

17. エンコーディング、暗号化モジュール（１８，１９，２０，２１，３５）は電子的データ処理回路の種々の個所に設けられていることを特徴とする請求の範囲１６記載のデータ処理回路。

【発明の詳細な説明】

電子的データ処理回路

本発明はマイクロプロセッサのような作動モジュールと、少なくとも１つのデータメモリと、データメモリと作動モジュールとの間に延びているデータバスとを有する電子的データ処理回路に関する。

上位概念による電子的データ処理回路は、屡々、安全上クリティカルな適用面にて使用される。ここで、データメモリ中には秘密のデータ、金額値及びアクセス使用権が格納され、それらは、作動モジュールにより、例えば外部の要求に基づき処理される。

当該のメモリは屡々、できるだけアクセスすべきでない情報を含むのであるから、従って、電気的データ処理回路の操作に対する安全手段を講ずる必要がある。

上位概念による電子的データ処理回路が集積化回路として構成されている場合、当該の集積化回路を種々のパッシベーション層で覆うことができる。ここで、パッシベーションを次のように施すことができる、即ち、パッシベーションを除去するとデータメモリの破壊が生ぜしめられるように施すことができる。更に、データメモリを集積化回路の比較的に深い層間に埋込み、その結果それに対するアクセスが困難化される。

電子的データ処理回路を不都合な操作から保護する更なる手法は、電子的データ処理回路の作動条件をスキャンするセンサの使用である。センサによりスキャンされた値が通常の値外に位置すると直ちに、相応の保護手段がトリガされ、この相応の保護手段により、電子的データ処理回路の非作動化又はデータメモリの消去が生ぜしめられる。

更に、禁止された命令に基づいての、又は規定に従っての作動に関して阻止されているアドレス領域に従っての作動モジュールの作動を監視するソフトウエアセンサも存在する。

更に、特別な作製モードで、作動モジュールの許容されたデータメモリへのメモリアクセスを、特別なハードウエア装置により、例えば分離可能に構成された

接続トラヒクにより制限することも公知である。

前述の安全保護手段にも拘わらず、上位概念による電子的データ処理回路での不都合な操作が時折なされる。

従って、本発明の課題とするところは、不都合な変更、変化をさせないような防止保護をするための改善された手段を有する上位概念による電子的データ処理回路を提供することにある。

前記課題は、本発明によれば、上位概念による電子的データ処理回路において次のようにして解決される、即ち、データメモリ）と、データバスとの間の領域

にて、及び／又は作動モジュールとデータバスとの間の領域にて少なくとも１つのエンコーディング、暗号化モジュールが設けられており、ここで前記エンコーディング、暗号化モジュールは、次のように構成されている、即ち作動モジュールとデータバスとの間の領域にて、ないし、データメモリと、データバスとの間の領域にて、エンコーディング、符号化及び／又はデコーディング、復号化が実施可能であるように構成されているのである。

本発明は、新たな技術的手法により、集積化回路として構成された電子的データ処理回路の操作性が容易化されているという本質的認識に立脚する。而して操作者の側から、データ処理回路は、集積化回路にてもはやそれの全体がチップとして見なすべきものではなく、コンポーネントに別個にアクセスできる、１つのシリコン担体上の個々のコンポーネントから成る１つのシステムと見なされるべきものである。

従って、データバス上でのデータトラヒックの観測により、又はデータメモリの読出により、データメモリ内に記憶された情報に対する推論を引き出し得、その結果操作が容易化される。

本発明の重要な認識によれば上位概念による電子的データ処理回路における多くの操作は次のことに帰せられ得る、即ち、データトラヒックをデータバス上で“モニタ盗聴”でき、その結果作動モジュールにおけ

るプログラムシーケンスが観測され、不都合に了解され得るということに帰せら

れ得る。

本発明によれば、データを電子的データ処理回路にてエンコーディングして転送し、ここで、データバスとデータメモリとの間でデータバス上で転送されるデータトラヒックエンコーディング、暗号化及びデコーディング、復号化するための手段が設けられる。その種の装置を以下“エンコーディング、暗号化モジュール”と称される。ここで、上記呼称は、たんにエンコーディングのみを実施する装置に限定されない。本発明の基本的技術思想によれば、前記呼称は、エンコーディング及び、デコーディングの双方、ないしそれらの両動作のうち、１つのみを実施する装置をも意味する。

本発明の電子的データ処理回路の構成によればデータバス上でのデータトラヒックを首尾よくトラッキングした場合でも、データメモリ内に記憶されたデータを直接推論できない。データメモリ内に記憶されたデータの読出が首尾よくいった場合でも、それの意味を引き出すことができない、それというのは予備知識のない者にとって何等意味のあるものと成り得ないからである。

ここで本発明によるエンコーディング、暗号化及びデコーディング、復号化がチップ全体に亘り分布され、ないし、ずらし、変位せしめられて行われるようにするとよい、それというのは、首尾よく行われる操作のためには、電子的データ処理回路の複数個所の同時観測が必要となるからであり、このことは、技術的に実施するのは唯困難であるからである。

データメモリへのアクセスの一時記憶のためラッチ一時メモリを備えた電子的データ処理回路の場合本質的なことは、エンコーディング、暗号化モジュールをラッチ一時メモリの内容が常にエンコーディングされているように構成されていることである。それというのは、ラッチの内容を比較的容易に観測でき、その結果、その内容は本発明のデータ処理回路の作動中、安全のためエンコーディングされねばならない。

エンコーディング、暗号化及びデコーディング、復号化は、本発明によりデータ処理回路のＣＰＵ内にまで及び得る。更に、エンコーディング、暗号化及びデコーディング、復号化を、相互に無関係に複数のエンコーディング、暗号化モジ

ュールにて行うこともできる。本発明によれば、唯一のエンコーディング、暗号化モジュールが設けられる手段も包括される。

更に、１つのマルチタスキング処理において種々のアプリケーションを処理するデータ処理回路においてさらに利点が得られる。その場合、適当なエンコーディングにより、種々のアプリケーションに、種々のデータメモリを対応付けでき、ここで各タスクに対して１つの異なるキー鍵が取り極められる。それにより、ある１つのタスクが、他のタスクにアクセスできないようになる。

要するに、本発明によれば、データ処理回路をたんに物理的にしらべるだけではもはや十分ではないようになる。付加的に、殊に、複数のコンポーネントの同時の観測下で単数ないし複数のエンコーディング、暗号化モジュール内に記憶されたキー鍵及び場合により当該キー鍵の動作も識別されねばならない。

本発明の構成形態では、エンコーディング、暗号化モジュールは、データトラヒックがエンコーディングアルゴリズムを用いてエンコーディング可能であるように構成されるのである。そのように構成されたエンコーディング、暗号化モジュールにより得られる利点とするところは、量産の場合殊に有利なコストで作製可能であることである。但し、アルゴリズムでのエンコーディングは、極めて長時間継続する、それというのは、それにより、作製モジュールにおける広汎な計算が必要になるからである。従って、その種の本発明によるデータ処理回路の実時間作動は、現在のところ未だ可能になっていない。

本発明によれば、エンコーディング、暗号化モジュールは、データトラヒックがハードウエアーエンコーディングを用いてエンコーディング可能であるように構成されている。まさにハードウエアーエンコーディングの場合、本発明のデータ処理回路の作動は、実時間で既に簡単に実現でき、而も、データメモリへの読出－及び書込アクセスの双方の場合に実現できる。

ハードウエアーエンコーディングを本発明により、エンコーディングモジュールで実施することができ、このモジュールは、データトラヒックにおける個々の

ビットのウエイトが選択的に変化可能であるように構成されているのである。その場合メモリ中で例えば“Ｌｏｗ”として格納されたビットはデータトラヒック中、データバス上で“Ｈｉｇｈ”として現れる。このことは例えばエンコーディング、暗号化モジュールで行い得、エンコーディング、暗号化モジュールは、少なくとも１つのＥＸＯＲ素子を有するのである。

本発明のさらなる実施形態によれば、エンコーディング、暗号化モジュールは、データバスのデータ線路の接続シーケンスが選択的に変化可能であるように構成されているのである。このことは、データバスの個々のビット線路が入れ替わったかのように外部に向かって現れる。

更に、本発明のデータ処理回路におけるハードウエアーエンコーディングをエンコーディングモジュールで実施することもでき、このモジュールは、データバスと作動モジュールとの間、及び／又はデータバスとデータメモリとの間でのデータトラヒックが少なくとも部分的に選択的に遅延可能であるように構成されているのである。それにより、データバス上で本発明によ

る電子的データ処理回路の瞬時の作動状態に関連のないデータトラヒックがシミュレートされる。

ここで本発明のデータ処理回路の１つの重要な構成要件によれば、エンコーディング、暗号化モジュールを次のように構成する、即ち、エンコーディングが選択的に動作するように構成するのである。つまり、エンコーディングは選択的に行われたり、又は行われなかったりする。更にこのことは次のようにしても行われる、即ち、データトラヒックのエンコーディングのため種々のキー鍵間で切換を行い得るのである。この場合においても本発明のエンコーディング、暗号化モジュールの使用上ダイナミック特性が得られる。

まさに、キー鍵の切換わる本発明のデータ処理回路の場合において、１つのバッチ、ないし、１つの作製ロットの各データ処理回路がそれぞれ異なる個別のキー鍵を有するようにする。それにより、１つのデータ処理回路のキー鍵を知得しても、他のデータ処理回路のキー鍵を推論できないことが確保される。

本発明の実施形態によれば．エンコーディング、暗号化モジュールは少なくと

も１つのキー鍵の入力のために少なくとも１つの入力側を有するのである。エンコーディング、暗号化モジュールにおける当該の入力側は、エンコーディング、暗号化モジュール自体にて記憶された所定のキー鍵間で、そしてさらにエンコーディング、暗号化モジュールにて使用されたエンコー

ディングプロセス間で切換えを行うためにも使用できる。また、単一のエンコーディングプロセスを作動し、ないし非作動化することも簡単に可能になる。それと異なって、外部に記憶されたキー鍵を入力することもできる。このために、キー鍵は有利にフラッシュ（ＦＬＡＳＨ）セル又はＥＥＰＲＯＭセル内に記憶される。前述のセルは、比較的確実であると見なされる、それというのは、フローティングゲート上の情報は、たんに“わずかな”電子で記憶されるからである。それの内容を読み出す大抵の試行は、記憶された情報を破壊する。従って、本発明の実施形態によれば、データトラヒックの確実なエンコーディングが可能になる。更に、すべてのＦＬＡＳＨ－セルは、プログラミング可能性の利点がある。而して、簡単な方法で本発明のデータ処理回路の供給引き渡しの際、各回路内に、個別のキー鍵をプログラミングし、さらなる変更に対して阻止できる。

次のようにすれば安全確実性のさらなる改善が可能になる、即ち、キー鍵は、データ処理回路の収容のためＩＣ回路の埋込構造内に埋込まれているのである。ここで、集積化モジュールは有利に、データ処理回路をも収容する。埋込まれた構造は、分散的に集積化回路の種々の個所に実施できるという利点がある。これにより、確実性が著しく高められる、それというのは、１つの集積化回路内に収容されたデータ処理回路の

種々の個所を同時に観測することが困難であるからである。更に、キー鍵の格納された場所の操作をスキャンするセンサを設けることもでき、本発明のデータ処理回路をこの場合に対して、非作動化にし、又は使用不能にし得る。

本発明によるデータ処理回路の作製の際、記憶されるキー鍵と代替選択的にそれによりキー鍵をランダムに選択できるランダム発生器を設けることができる。

本発明の特に有利な構成形態では、エンコーディング、暗号化モジュールにて

使用されるキー鍵の選択が、作動モジュールにより、殊に、プログラムシーケンス中実施される。このために本発明の実施形態によれば、データ処理回路は次のように構成されている、即ち、作動モジュールにより、所定の動作の実施の際、１つのキー鍵がエンコーディング、暗号化モジュール内に入力可能であるように構成されている。作動モジュールのプログラムコードは、場合により知られているので、キー鍵選択は有利に通常のプログラムコード内に隠されて行われる。而して、作動モジュールは、例えば次のように構成され得る、即ち有害でない、ないし差し障りのない命令、例えばＣＬＲ　Ｃ（“ＣＬＥＡＲ　ＣＡＲＲＹ）の実行の際、単数又は複数のエンコーディング、暗号化モジュールのキー鍵が切換えられるように構成され得る。

更に、時間測定装置を設けてもよく、該時間測定装

置は、キー鍵の入れ替えを監視し、キー鍵の入れ替えをトリガすることもできるのである。。

エンコーディング、暗号化モジュール内に使用されるキー鍵に関して、キー鍵が作動モジュールないしＣＰＵにより生ぜしめられるようにするとよい。このことは、例えばＣＰＵにより生成されるアドレスから変換プロセスによりキー鍵の導出により行われる。当該プロセスの利点とするところは、キー鍵が絶えず、即ち各アドレスごとに変化することである。種々の変換方法の選択により、作動モジュールのプログラマがエンコーディングへ影響を及ぼし得る。このことは、例えばＣＰＵにより生成されるアドレスから変換プロセスによりキー鍵の導出により行われる。当該プロセスの利点とするところは、キー鍵が絶えず、即ち、各アドレス語とに変化することである。種々の変換方法の選択により、作動モジュールのプログラマがエンコーディング、暗号化に影響を及ぼし得る。

要するに、データトラヒックが本発明のデータ処理回路にて次のような場合のみ操作者により了解され得るようにするとよい、即ち、その都度エンコーディング、暗号化モジュールにて使用されているキー鍵が知られている場合のみ操作者により了解され得るようにするとよい。データメモリ内に格納されたデータも、データメモリに所属するキー鍵の知得下でのみ了解され得る。このことは、操作

に対する安全防止機能が高

いからである。

勿論データ処理回路の作動モジュールをプログラミングしたプログラマは、キー鍵に所属するデータのうちどれが、データメモリないしデータ処理回路のどのアドレスのうちに格納しているかの秘密のリストを作らなければならない。キー鍵の種類に応じてプログラマは、所定の充足すべき前提条件を設定するとよく、この前提条件は、例えば、常に値対を読出さなければならないことに表される。

本発明の電子的データ処理回路の特に有利な実施形態によれば、作動モジュール及び少なくとも１つのデータメモリを結合するデータバスの少なくとも１つのデータ線路の領域にて、少なくとも２つのエンコーディング、暗号化モジュールが設けられており、ここで、前記エンコーディング、暗号化モジュールは、次のように構成されている、即ち、エンコーディング、暗号化モジュールの共働により完全なエンコーディング、暗号化及びデコーディング、復号化が実施可能であるように構成されているのである。有利にはエンコーディング、暗号化モジュールは、電子的データ処理回路の種々の個所に設けられているのである。当該の構成形態により、データトラヒックのエンコーディング、暗号化が２つの異なった個所でエンコーディング、暗号化が確保される。典型的な操作者は、おそらく唯一のエンコーディング、暗号化を唯一の個所にて、即

ち単一のエンコーディング、暗号化モジユールにて実施し、エンコーディング、暗号化の適用の際有用な結果に立至らないであろう。異なる個所に収容された２つのエンコーディング、暗号化モジュールを有する実施例の場合、エンコーディング、暗号化を実施するのが特に困難である、それというのは１つの、マイクロ構造の２つの異なる個所を同時に観測するのは特に困難だからである。そのような構成されたエンコーディング、暗号化モジュールは、例えば次のように構成し得る、即ち、１つのエンコーディング、暗号化モジュールが、１つの個所にて、１つのデータバスの、下方の４つのビットをエンコーディング、暗号化ないしデコーデイング、復号化し、これに対し、他方のエンコーディング、暗号化モジュ

ールがデータバスの残りのビットをエンコーディング、暗号化ないしデコーディング、復号化するように構成し得る。

本発明の手法のさらなる利点とするところは、次のような上位概念によるデータ処理回路において得られる、即ち、相互に交信し得るのは、データ処理回路のすべてのコンポーネントではないような上位概念によるデータ処理回路において得られる。その際キー鍵の適当な構成により、たんにそのために設けられたデータバスの接続経路においてのみ例えば所定数のエンコーディング、暗号化ユニットと交信し得る。適当でないエンコーディング、暗号化を有する他のすべての接続は適切に機能し得ない。

本発明を２つの簡単な実施例及び１つの複雑な実施例に即して説明する。

図１は、ＣＰＵにおいて、単一のエンコーディング、暗号化装置を有する本発明の電子的データ処理回路を示し、

図２は、図１の電子的データ処理回路の変形を示し、

図３は、ＣＰＵ及びデータメモリの領域におけるエンコーディング、暗号化装置付きの本発明の電子的データ処理回路を示す。

図１は、作動モジュールとして１つのＣＰＵ１０１及び複数のデータメモリとして本発明のデータ処理回路を示す、詳細に云えば、これは、ＲＯＭ１０２，ＥＥＰＲＯＭ１０３，フラッシュ（ＦＬＡＳＨ）メモリ１０４，ＲＡＭ１０５である。データメモリ１０２～１０５及びＣＰＵ１０１は、データバス１０６を介して相互に接続されている。

ＣＰＵ１０１では、エンコーディング、暗号化モジュール１０７が設けられており、該エンコーディング、暗号化モジュール１０７は、ＣＰＵ１と、データメモリ１０２～１０５との間のデータトラヒックをエンコーディング、暗号化及びデコーディング、復号化する。ここで再度指摘すべきことには、その種の装置は、以降“エンコーディング、暗号化モジュール”と称され、たんに、エンコーディング、暗号化のみを実施する装置に限定されるものでない。本発明の基本的技術思想によれば、当該の呼称により、エンコーディン

グ、暗号化のみならず、デコーディングをも、ないしそれら両動作のうちの１つのみを実施する装置を意味する。ここで、エンコーディング、暗号化ないしデコーディング、復号化を、適当な遅延により、データバスのビット線路の入れ替えにより、又は個々のデータビットのウエイト変更、変化により行うことができる。ホソフトウエアーエンコーディング、暗号化を実施することもできる。

更に本発明のデータ処理回路は、マルチプレクサ１０８を有し、該マルチプレクサは、データ線路１０９を介してフラッシュ（ＦＬＡＳＨ）メモリ１０４と接続されている。マルチプレクサは、データ線路１１０を介してタイマ１１１と接続されており、タイマ１１１には、データ線路１１２を介してランダム発生器１１３からランダム数が供給可能である。マルチプレクサ１０８は、制御線路１１４をも有し、該制御線路１１４を介して、ＲＯＭ１０２と接続されている。更にマルチプレクサ１０８へのリセットＲＥＳＥＴ線路１１５が設けられており、該リセットＲＥＳＥＴ線路を介して、マルチプレクサ１０８がデータ処理回路のリセットの際基本状態へリセット可能である。マルチプレクサ１０８の出力側は、制御線路１１６を介してエン

コーディング、暗号化モジュール１０７と接続されており、ここでエンコーディング、暗号化モジュール１０７は、マルチプレクサ１０８の出力信号に基づき新たなキー鍵を供給される。本発明によれば、エンコーディング、暗号化モジュール１０７にて、制御線路１１６を介するマルチプレクサ１０８の出力信号に基づき、エンコーディング、暗号化モジュール１０７にて使用されているエンコーディング、暗号化プロセス方式が切換られる。

動作中、本発明の電子的データ処理回路は、次のように動作する。プログラムスタート（ＲＥＳＥＴ）の際、マルチプレクサにてリセット線路１１５上の信号に応答してスタートキー鍵が調整セッティングされる。ついで、データバス１０６とＣＰＵ１０１との間のデータトラヒックが、エンコーディング、暗号化モジュール１０７にてエンコーディング、暗号化ないしデコーディング、復号化され、ここで、エンコーディング、暗号化モジュール１０７を通ってデータが貫通するごとに、相応の動作ないし演算がデータ流方向に相応して実施される。命令“

ＣＬＲ　Ｃ”の実行ごとに、ＲＯＭ１０２は制御線路１１４を介して１つの制御パルスをマルチプレクサ１０８へ伝送する。ついでマルチプレクサ１０８は、データ線路１０９を介してフラッシュ（ＦＬＡＳＨ）メモリ１０４から３つのキー鍵ＫＥＹ３，ＫＥＹ２，ＫＥＹ１のうちの１つを取出

し、これをエンコーディング、暗号化モジュール１０７に伝達する。エンコーディング、暗号化モジュール１０７にて使用されたキー鍵が交換され、又は、制御線路１１６上にて加わっている信号のウエイトに応じてエンコーディング、暗号化モジュール１０７にて使用されているエンコーディング、暗号化プロセス間で切換がなされる。マルチプレクサ１０８がＲＯＭ１０２により作動されないままデータ処理回路の所定の作動時間を超過したとき、タイマ１１１は動作する。タイマ１１１の作動により、マルチプレクサ１０８に、データ線路１１０を介して、ランダム発生器１１３からの１つのランダム数が伝達される。次いで、マルチプレクサ１０８は、ランダム数を、エンコーディング、暗号化モジュール１０７へ伝達する。

データメモリ１０２～１０５におけるデータは、エンコーディング、暗号化されて格納されている。従って、データは、データバス１０６上でエンコーディング、暗号化された状態でＣＰＵ１０１へ転送され、そこで、エンコーディング、暗号化モジュール１０７により再びデコーディングされる。その後はじめて、データはエンコーディング、暗号化されてない状態で、ＣＰＵにて処理され得る準備状態におかれている。

図２は、図１のデータ処理回路の変形を示し、このデータ処理回路は、同様に作動モジュールとしてＣＰＵ１０１及び複数のデータメモリを有する。詳細に云

えば、ＲＯＭ１０２，ＥＥＰＲＯＭ１０３，フラッシュ（ＦＬＡＳＨ）メモリ１０４及びＲＡＭ１０５がある。データメモリ１０２～１０５及びＣＰＵ１０１はデータバス１０６を介して相互に接続されている。

ＣＰＵ１０１には、エンコーデイング、暗号化モジュール１０７が設けられており、エンコーディング、暗号化モジュール１０７は、ＣＰＵ１と、データメモ

リ１０２～１０５と間でデータトラヒックをエンコーディングないし、デコーディングする。

図２のデータ処理回路は、図１のそれと異なって、エンコーディング、暗号化モジュール１０７に新たなキー鍵を供給するためのマルチプレクサを有しない。その代わり、図２のデータ処理回路は、制御線路１２２を介して変換モジュール１２０に接続されており、該変換モジュール１２０は、ＣＰＵ１０１のアドレスバス１２１と接続されている。この変換モジュールのアドレスバス１２１にはさらなる制御線路１２３が達しており、該さらなる制御線路１２３により、変換モジュール１２０内にて記憶された“アドレス”から“キー鍵”への種々の選択対象の複数変換のうちからの１つの所定の変換が選択できる。それにより、変換モジュール１２０により１つのキー鍵が、ＣＰＵ１０１にて加わっているアドレスから導出される。

動作中、図２の電子的データ処理回路は、実質的に図１のそれと同じ特性を有する。プログラムスタート

（ＲＥＳＥＴ）の際、１つのスタートキー鍵は、エンコーディング、暗号化モジュール１０７にて制御線路１２３上の１つの信号に調整セッティングされる。次いで、データバス１０６とＣＰＵ１０１との間の各データトラヒックが、エンコーディング、暗号化モジュール１０７でエンコーディング、暗号化ないしデコーディング、復号化され、ここで、エンコーディング、暗号化モジュールを通ってのデータの通過ごとに相応の動作ないし演算がデータ流方向に相応して実施される。制御線路１２３の作動ごとに、変換モジュール１２０は新たな変換に基づき１つのキー鍵を、ＣＰＵ１０１にて加わるアドレスから１つのキー鍵を導出する。

データメモリ１０２～１０５におけるデータは常にエンコーディング、暗号化されている。従って、データバス１０６上のデータは、エンコーディングされた状態でＣＰＵ１０１へ転送される。そこで、エンコーディング、暗号化モジュール１０７により再びデコーディングされる。その後はじめてデータはエンコーディング、暗号化されていない状態でＣＰＵにて処理され得る準備状態におかれて

いる。

図３の本発明のデータ処理回路は、作動モジュールとしてのＣＰＵ１及び複数のデータメモリを有する。詳しく云えば、ＲＯＭ２，ＥＥＰＲＯＭ３，フラッシュ（ＦＬＡＳＨ）メモリ４及びＲＡＭ５である。デー

タメモリ２～５及びＣＰＵ１は同図には示されていないデータバスを介して相互に接続されてている。データバスの代わりに、同図中、個々のデータ線路６～１５が設けられており、該個々のデータ線路を介して、ＣＰＵ１はデータメモリ２～５とデータを交換する。ＣＰＵ１とＲＯＭ２，ＥＥＰＲＯＭ３，フラッシュ（ＦＬＡＳＨ）４及びＲＡＭ５と間に更に各ラッチ一時メモリ１６～１９が設けられている。

ＲＯＭ２とラッチ１６との間の領域にて、ラッチ１７とＣＰＵ１との間の領域にてタッチ１８，１９とＣＰＵ１との間の領域にて並びにＣＰＵ１自体内にてエンコーディング、暗号化モジュール２０～２２及び３５が設けられている。該エンコーディング、暗号化モジュール２０～２２及び３５は、それに配属されたデータ線路上でのデータトラヒックをエンコーディング、ないし、デコーディングする。ここで再度指摘すべきことはその種の装置を以下“エンコーディング、暗号化モジュール”と称されるが、この“エンコーディング、暗号化モジュール”はたんにエンコーディング、暗号化のみを実施する装置に限られない。本発明の基本的技術思想によれば、当該の呼称により、エンコーディングのみならず、デコーディングをも、ないしそれら両動作のうちの１つのみを実施する装置をも意味する。ここで、エンコーディング、暗号化ないしデコーディング、復号化を、適当な遅延により、データ

線路のビット線路の入れ替えにより、又は個々のデータビットのウエイトの変更、変化により行うことができる。亦ソフトウエアーエンコーディング、暗号化を実施することもできる。

エンコーディング、暗号化モジュール２０～２２及び３５は次のように構成されている、即ちそれに配属されたデータ線路上でデータトラヒックがたんに部分

的にその都度エンコーディング、暗号化ないしデコーディング、復号化されるように構成されている。完全なエンコーディング、暗号化ないしデコーディング、復号化は、エンコーディング、暗号化モジュール２０、２１、２２のうちの各１つとエンコーディング、暗号化モジュール３５との共働の際はじめて行われ得る。

更に本発明のデータ処理回路は、マルチプレクサ２３を有し、該マルチプレクサは、データ線路２４を介してフラッシュ（ＦＬＡＳＨ）メモリ４と接続されている。マルチプレクサ２３は、データ線路２５を介してタイマ２６と接続されており、タイマ２６には、データ線路２７を介してランダム発生器２８からランダム数が供給可能である。マルチプレクサ２３は、制御線路２９をも有し、該制御線路２９を介して、ＲＯＭ２と接続されている。

マルチプレクサ２３の出力側は、制御線路３０～３４を介してエンコーディング、暗号化モジュール２０、２１、２２、３５と接続されており、ここでエンコーディング、暗号化モジュール２０、２１、２２、３５は、マルチプレクサ２３の出力信号に応答して新たなキー鍵を供給される。

動作中本発明のデータ処理回路は、次のように動作する。命令“ＣＬＲ　Ｃ”の実行ごとに、ＲＯＭ２は制御線路２９を介して１つの制御パルスをマルチプレクサ２３へ伝送する。ついでマルチプレクサ２３は、データ線路２４を介してフラッシュ（ＦＬＡＳＨ）メモリ４から３つのキー鍵ＫＥＹ３，ＫＥＹ２，ＫＥＹ１のうちの１つを取出し、これをエンコーディング、暗号化モジュール２０、２１、２２、及び２５に伝達する。データ処理回路の所定の作動時間を超過したときその際マルチプレクサ２３がＲＯＭ２により作動されない場合、タイマ１１１は動作する。タイマ１１１の作動により、マルチプレクサ２３に、データ線路１１０を介して、ランダム発生器１１３からの１つのランダム数が伝達される。次いで、マルチプレクサ２３は、ランダム数を、エンコーディング、暗号化モジュール１０７へ伝達する。

ＲＯＭ２におけるデータは、エンコーでぃング、暗号化された状態で格納されており、そして、ラッチ１６にて読み出し中、エンコーディング暗号化モジュ

ール２０により単に部分的にデコーディングされる。従って、　ＲＯＭ２からのデータは、データ線路６上でなお部分的にエンコーディング暗号化されてＣＰＵ

１へ転送され、そこで、エンコーディング、暗号化モジュール３５により完全にデコーディングされる。その後はじめて、データはエンコーディング、暗号化されずに、ＣＰＵにて処理され得る準備状態におかれている。

ＥＥＰＲＯＭ３にてエンコーディングされた状態で設けられたデータはデータ線路９を介してラッチ１７に伝送され、そこからエンコーディング、暗号化モジュール２１へ転送され、そこで、部分的にデコーディングされる。そこかから、なお部分的にエンコーディング、暗号化されたデータが、データ線路１１を介してＣＰＵ１へ達し、そこでエンコーディング、暗号化モジュール３５により完全にデコーディングされ、しかる後処理され得る準備状態におかれる。

フラッシュ（ＦＬＡＳＨ）メモリ４及びＲＡＭ５に対するデータは、完全にエンコーディング、暗号化された状態でフラッシュ（ＦＬＡＳＨ）－メモリ４にて又はＲＡＭ５にて記憶される前に先ず、その都度部分的にエンコーディング、暗号化モジュール３５及びエンコーディング、暗号化モジュール２２によりエンコーディングされる。このために、ＣＰＵ１のエンコーディング、暗号化モジュール３５にて部分的にエンコーディングされたデータがデータ線路１１を介してエンコーディング、暗号化モジュール２２へ伝送され、そこで完全にエンコーディング、暗号化されるが、そ

の前に、データ線路１３及び１４を介して、フラッシュ（ＦＬＡＳＨ）４及びＲＡＭ５に所属するラッチ１８，１９へ転送される。ラッチ１８，１９からエンコーディングされたデータがデータ線路１２，１５を介してフラッシュ（ＦＬＡＳＨ）メモリ４ないしＲＡＭ５へ達する。

フラッシュ（ＦＬＡＳＨ）メモリ４及びＲＡＭ５からのデータの読出の際、当該データはその都度部分的にエンコーディング、暗号化モジュール２２及びエンコーディング、暗号化モジュール３５によりデコーディング、復号化され、その前に完全にデコーディング、復号化されてＣＰＵ１にて処理され得る準備状態に

おかれる。

【図１】

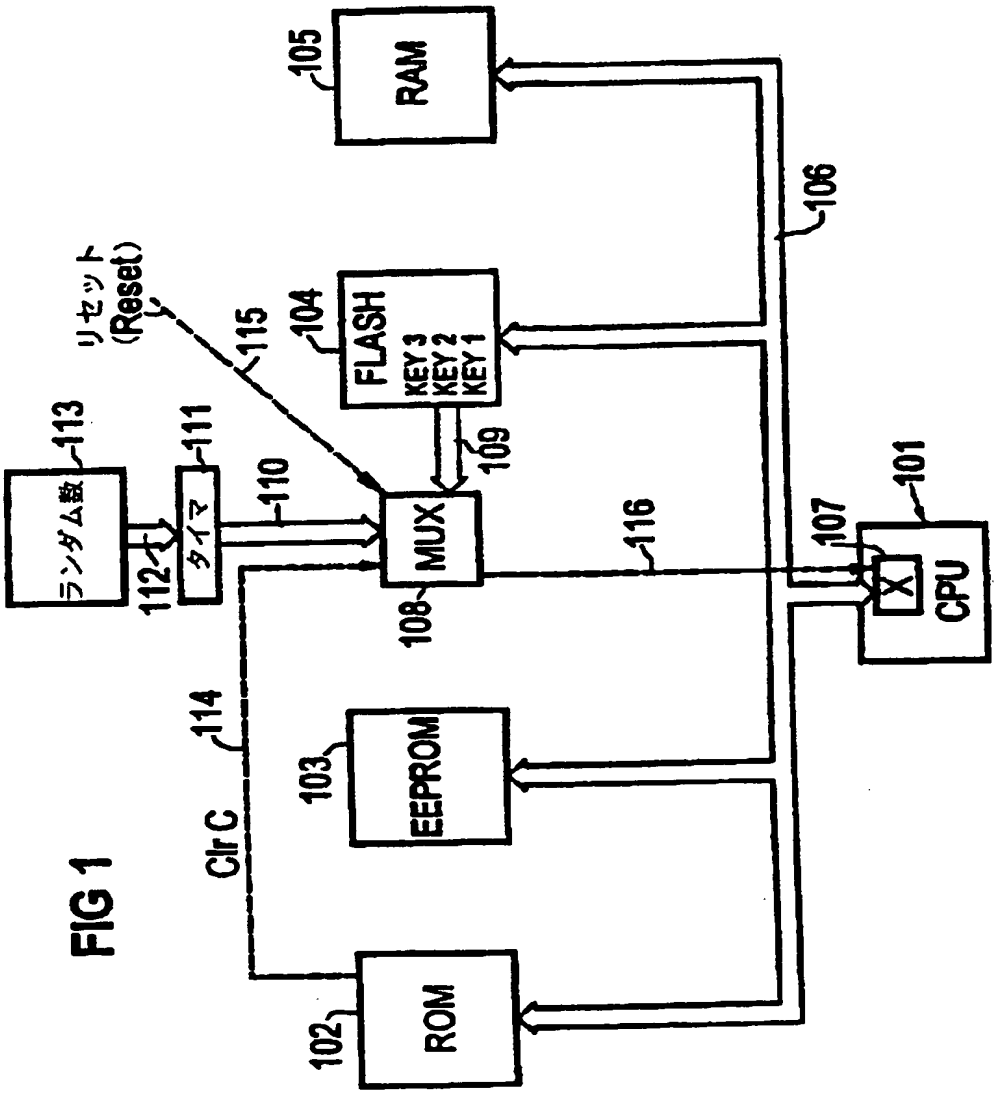
105
RAM
106
リセット
(Reset)
115
104
FLASH
KEY 3
KEY 2
KEY 1
113
111
109
101
ランダム数
タイマ
110
MUX
116
107
CPU
112
108
114
103
EEPROM
Clr C
102
ROM

FIG 1

【図２】

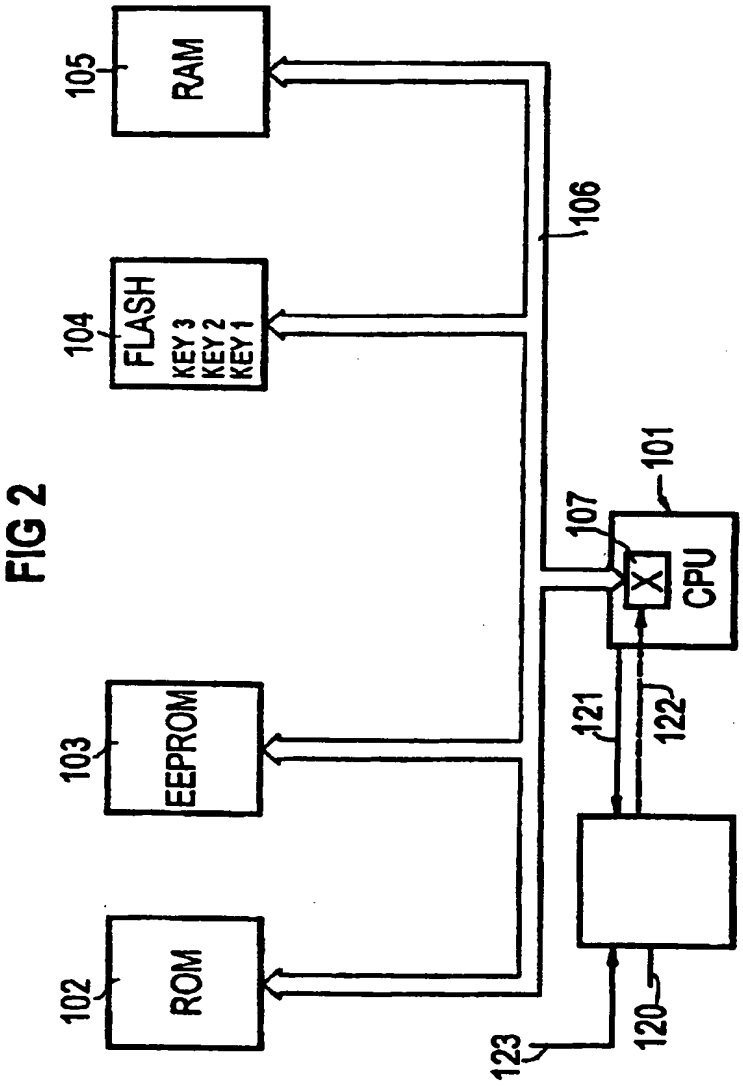
105
RAM
106
104
FLASH
KEY 3
KEY 2
KEY 1
101
107
X
CPU
103
EEPROM
121
122
102
ROM
123
120

FIG 2

【図３】

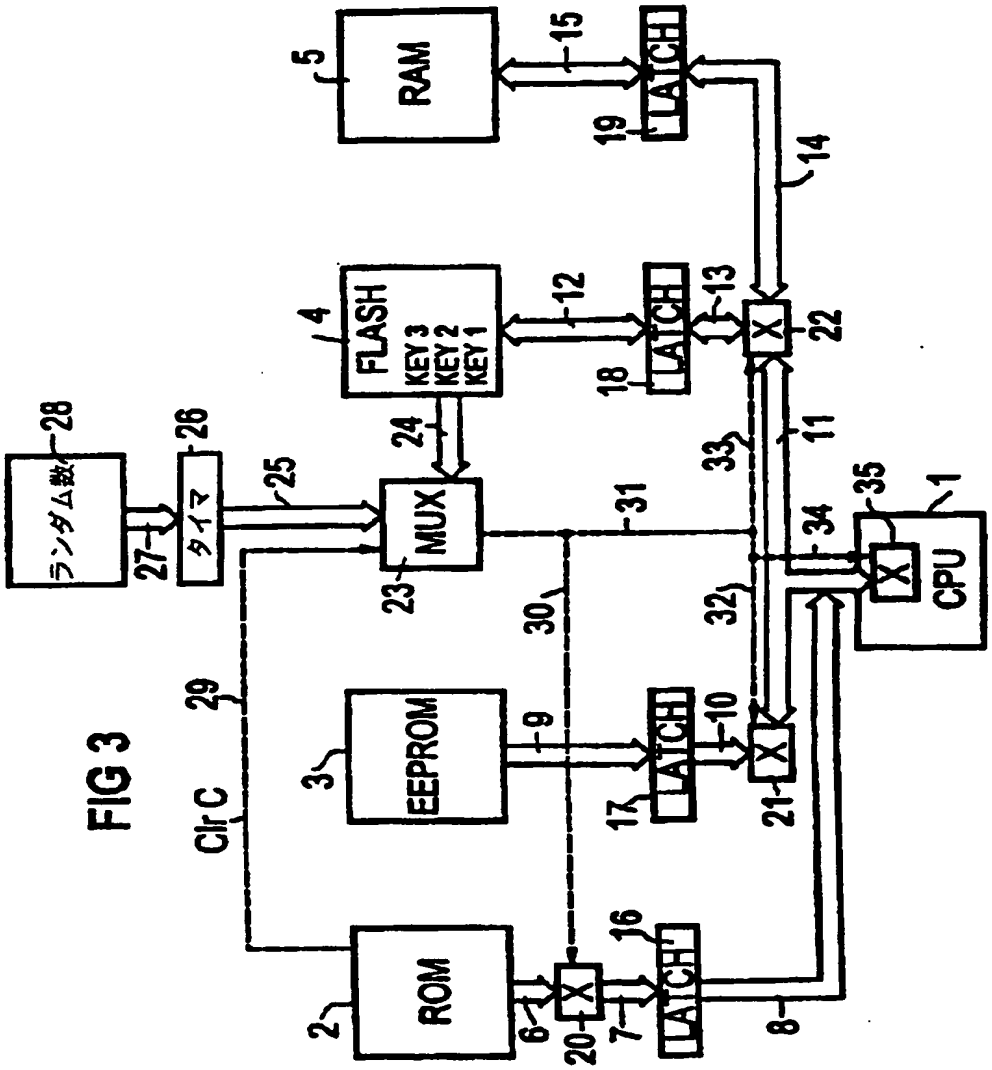
RAM
5
15
19
LATCH
14
FLASH
KEY 3
KEY 2
KEY 1
4
12
18
LATCH
13
X
22
11
33
28
ランダム数
26
タイマ
27
25
24
MUX
23
31
35
1
CPU
34
32
30
29
EEPROM
3
9
LATCH
10
17
X
21
Clr C
ROM
2
6
X
20
7
16
LATCH
8

FIG 3

【手続補正書】特許法第１８４条の８第１項

【提出日】１９９８年５月２３日（１９９８．５．２３）

【補正内容】

請求の範囲

1. マイクロプロセッサのような作動モジュールと、少なくとも１つのデータメモリと、データメモリと作動モジュールとの間に延びているデータバスとを有する電子的データ処理回路において、

作動モジュール（１）及び少なくとも１つのデータメモリ（２，３，４，５）を接続するデータバスの少なくとも１つのデータ線路（７，８，３４，１１）の領域にて少なくとも２つのエンコーディング、暗号化モジュール（１８，１９，２０，２１，３５）が設けられており、ここでエンコーディング、暗号化モジュール（１８，１９，２０，２１，３５）は、次のように構成されている、即ちエンコーディング、暗号化モジュール（１８，１９，２０，３５）の共働により完全なエンコーディング及び／又はデコーディングが実施可能であるように構成されていることを特徴とする電子的データ処理回路。

2. エンコーディング、暗号化モジュール（１８，１９，２０，２１，３５，）は電子的データ処理回路の種々の個所に設けられていることを特徴とする請求の範囲１記載のデータ処理回路。

3. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックがエンコーディングアルゴリズムを用いてエンコーディング可能であるように構成されていることを特徴とする請求の範囲１又は２記載のデータ処理回路。

4. エンコーディング、暗号化モジユール（２０，２１，２２，３５，１０７）は、データトラヒックがハードウエアエンコーディング、暗号化を用いてエンコーディング可能であるように構成ことを特徴とする請求の範囲１から３までのうち１項記載のデータ処理回路。

5. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックの個々のビットのウエイトが選択的に変化可能であるよ

うに構成されていることを特徴とする請求の範囲１から４までのうちいずれか１項記載のデータ処理回路。

6. エンコーディング、暗号化モジュールは、少なくとも１つのＥＸＯＲ素子を有することを特徴とする請求の範囲５記載のデータ処理回路。

7. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データバスのデータ線路の接続シーケンスが選択的に変化可能であるように構成されていることを特徴とする請求の範囲１から６までのうち１項記載のデータ処理回路。

8. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は、データトラヒックが少なくとも部分的に遅延可能であるように構成されていることを特徴とする請求の範囲１から７までのうち

いずれか１項記載のデータ処理回路。

9. エンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）は少なくとも１つのキー鍵の入力のために少なくとも１つの入力側を有することを特徴とする請求の範囲１から８までのうち１項記載のデータ処理回路。

10. １つ又は複数のキー鍵がデータ処理回路の１つのフラッシュ（Ｆｌａｓｈ）－セル内に格納されていることを特徴とする請求の範囲９記載のデータ処理回路。

11. キー鍵は、データ処理回路の収容のためＩＣ回路の埋込構造内に埋込まれていることを特徴とする請求の範囲９又は１０項記載の装置。

12. キー鍵がそこに格納されている場所の操作スキャニングのためにセンサ系が設けられていることを特徴とする請求の範囲９又は１０記載のデータ処理回路。

13. データ処理回路は次のように構成されている、

即ち、作動モジュールにより、所定の動作実施の際、１つのキー鍵がエンコーディング、暗号化モジュール（２０，２１，２２，３５，１０７）内に入力可能であることを特徴とする請求の範囲９から１２までのうち１項記載のデータ処理回路。

14. ランダム発生器（２８）が設けられており、該ランダム発生器（２８）により、１つのキー鍵がラン

ダムに選択可能であることを特徴とする請求の範囲９から１３までのうち１項記載のデータ処理回路。

15. 作動モジュール（１０１）にて使用されているアドレスから１つのキー鍵を導出するための装置（１２０）が設けられていることを特徴とする請求の範囲９から１４までのうち１項記載のデータ処理回路。

16. 時間測定装置（２６）が設けられており、この時間測定装置（２６）により、キー鍵の入れ替えが導入可能であることを特徴とする請求の範囲９から１４までのうち１項記載のデータ処理回路。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/DE 97/02070

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 449 256 A (TOKYO SHIBAURA ELECTRIC CO ;TOSHIBA MICRO ELECTRONICS (JP)) 2 October 1991 see the whole document	1,3-5
Y	---	16,17
Y	GB 2 099 616 A (JPM AUTOMATIC MACHINES LTD) 8 December 1982 see the whole document	16,17
X	--- "SECTION 1: INTRODUCTION" DATA BOOK SOFT MICROCONTROLLER, 6 October 1993, pages 1-3, 7, 8, 73, 77-80, 82, 152-156, 229, 290-292, XP002053731	1,2
Y	---	3-6,8-15
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 1998	18/02/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/DE 97/02070

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 386 469 A (YEARSLEY GYLE ET AL) 31 January 1995 see abstract; figure 1	3-6,8-15
A	US 4 598 170 A (PIOSENKA GERALD V ET AL) 1 July 1986 see the whole document	6
A	WO 95 16238 A (TELEQUIP CORP) 15 June 1995 see abstract; figure 2 see page 2, line 14 - line 27 see page 4, line 29 - page 5, line 7	9

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/DE 97/02070

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0449256 A	02-10-91	JP 3276345 A	06-12-91
		DE 69126557 D	24-07-97
		DE 69126557 T	13-11-97
		US 5214697 A	25-05-93
GB 2099616 A	08-12-82	NONE	
US 5386469 A	31-01-95	NONE	
US 4598170 A	01-07-86	NONE	
WO 9516238 A	15-06-95	AU 1265195 A	27-06-95
		US 5623637 A	22-04-97

【要約の続き】
３５，１０７）が設けられており、ここで前記エンコーディング、暗号化モジュール（２０～２２，３５，１０７）は、次のように構成されている、即ち作動モジュール（１，１０１）とデータバス（１０６）との間の領域にて、ないし、データメモリ（２，３，４，５，１０２，１０３，１０４，１０５）と、データバス（１０６）との間の領域にて、エンコーディング、符号化及び／又はデコーディング、復号化が実施可能であるように構成されているのである。